IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF 10 DIGITAL DEVICES DESCRIBED IN ATTACHMENT A, CURRENTLY LOCATED AT FAIRFAX COUNTY POLICE DEPARTMENT, 10600 PAGE AVENUE, FAIRFAX, VIRGINIA 22030	**UNDER SEAL** Case No. 1:23-SW-008

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Matthew Lee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION & AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of electronic devices and forensic extractions from those devices, described further below and in Attachment A, that are currently in law enforcement possession, for the information and items described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so since 2017 and am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C). As part of my duties as a Special Agent, I am currently assigned to the FBI Washington Field Office's Child Exploitation and Human Trafficking Task Force. In my current assignment, I investigate violations of federal law, including the online sexual exploitation of children. This includes violations pertaining to the illegal possession, receipt, distribution, transmission, advertisement, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the detection and investigation of criminal offenses. I have written, executed, and/or participated in the execution

of numerous search warrants, including search warrants of digital devices. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained experience in these investigations through training and discussions with other law enforcement officers. As a federal agent, I am authorized to investigate violations of laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. The facts and information in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF DEVICES TO BE EXAMINED

4. The property to be searched (collectively, "the Devices"), as further described in Attachment A, include the following items and any forensic extractions of the Devices:

1. Dell Latitude laptop computer, serial number HCD9LQ1
2. Jitterbug cellular telephone[1]
3. ASUS Chromebook laptop computer, serial number K6NXCV038893237
4. Three universal serial bus (USB) flash drives
5. Samsung A12 cell phone
6. Western Digital Easystore hard drive, serial number WXP1AC9JKKSP
7. ASUS X541N laptop computer, serial HAN0GR01C57341C

[1] I know from my experience and from research I conducted on the Internet that Jitterbug phones are relatively simple cell phones that typically have large buttons and limited functionality to ensure easier use than more advanced cell phones. Some Jitterbug phones have cameras, memory that can store images and videos, and the ability to connect to the Internet.

8. 1 Gigabyte (GB) Micro secure digital (SD) card, model PNY

9. AT&T cellular telephone, model V102AA

10. Samsung SGH-A157V cellular telephone, serial number R21D90HMV3R

5. The Devices are currently located at the Fairfax County Police Department's office located at 10600 Page Avenue, Fairfax, Virginia 22030, within the Eastern District of Virginia.

6. The applied-for warrant would authorize the forensic examination of the Devices, as described in Attachment A, for the purpose of identifying electronically stored data particularly described in Attachment B.

7. The devices were originally seized from the owner by the Fairfax County Police Department (FCPD) pursuant to a residential search warrant issued by a Fairfax County Magistrate. Out of an abundance of caution, I am seeking an overlay search warrant to examine and search the Devices and to be certain that any examination of these items will comply with the Fourth Amendment and other applicable laws.

STATUTORY AUTHORITY

8. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibits the knowing possession or access with intent to view of one or more books, magazines, periodicals, films, or other materials which contain any visual depictions of minors engaged in sexually explicit conduct that have been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce, by any means, including by computer.

DEFINITIONS

9. The following definitions apply to this Affidavit and its Attachments:

a. Title 18, United States Code, Section 2256(1) defines "minor" as any person under the age of eighteen years.

b. Title 18, United States Code, Section 2256(8) defines "Child Pornography" in relevant part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where … the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct."

c. Title 18, United States Code, Section 2256(2) defines "sexually explicit conduct" as actual or simulated: (i) Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) Bestiality; (iii) Masturbation; (iv) Sadistic or masochistic abuse; or (v) Lascivious exhibition of the anus, genitals or pubic area of any person.

d. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

e. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the Internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

10. Information set forth elsewhere in this Affidavit establishes that the owner of the Devices has a sexual interest in children and in sexually explicit images and videos of children and is a collector of child pornography. My knowledge of these types of individuals and their characteristics is based on my experience as an FBI agent and the training I have received focused on crimes against children. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics, which may be exhibited in varying combinations:

11. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

12. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

13. Likewise, individuals who have a sexual interest in children or images of children often maintain their "hard copies" of child pornographic material, that is, their pictures, films,

videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location, such as their personal cellular phone, or on their person. Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a cellular phone or on their person, allows persons who exploit children the opportunity to safely maintain their collections for many years and enable them to frequently view the materials, which are valued highly.

14. People with a sexual interest in children often transfer child pornographic material to multiple electronic devices because they value it so highly and because this transfer is sometimes necessary to create additional storage space. Additionally, because persons who collect child pornography are often compulsive about their activity, they often use multiple electronic devices throughout a home to access material depicting children or to communicate with children, especially when they have resided in the same place for a long period of time. Child pornography images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images/videos can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to offices, storage facilities, garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

15. Persons who collect child pornography may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, cellular telephone, and in person.

16. Based on my above knowledge about individuals with a sexual interest in children and the facts in the affidavit outlined below, there is probable cause to believe that the Defendant is a collector of child pornography and that his Devices and their forensic extractions contain evidence of the Defendant's sexual interest in children as well as his receipt and possession of child pornography.

SUMMARY OF PROBABLE CAUSE

13. This investigation involves David **SOLOMON** and his use of the Devices to possess images and videos depicting minors engaging in sexually explicit conduct.

14. In 2011, **SOLOMON** was convicted in Fairfax County Circuit Court of possessing child pornography in violation of § 18.2–374.1:1 of Virginia Code. Accordingly, **SOLOMON** is a registered sex offender. **SOLOMON** initially registered with the Virginia State Police as a sex offender on May 15, 2011. **SOLOMON** renewed his registration as recently as May 6, 2020.

15. Because of his status as a registered sex offender, **SOLOMON** is currently on active probation with the Virginia Department of Corrections (VADOC).

16. On November 28, 2022, VADOC Probation and Parole Officer (PO) Samluk visited **SOLOMON**'s home at 1808 North Shore Court, Reston, Virginia, within the Eastern District of Virginia, pursuant to the terms of **SOLOMON**'s supervised release conditions.

17. During this home visit, PO Samluk observed three laptops and multiple hard drives in **SOLOMON**'s possession. While speaking to PO Samluk about these devices, **SOLOMON** informed PO Samluk that he (**SOLOMON**) maintained adult pornography on at least some of the Devices. Later in the visit, **SOLOMON** told PO Samluk that he (**SOLOMON**) maintained child pornography on at least some of the Devices as well. For example, **SOLOMON** advised that one of his laptop computers contained over 100 images of child pornography.

18. Based on these facts, on November 28, 2022, while PO Samluk was at **SOLOMON**'s residence, FCPD Detective and FBI Task Force Officer Blake Allbritton sought a search warrant for **SOLOMON**'s residence. On that same date, a Fairfax County Magistrate issued the requested warrant ("the Fairfax County warrant").

19. On November 28, 2022, FCPD personnel executed the search warrant at **SOLOMON**'s residence and recovered the Devices, which are further described in Attachment A. The Defendant admitted that each of the Devices were his. All of the Devices were recovered from **SOLOMON**'s residence at 1808 North Shore Court, Reston, Virginia, which is also the address on his Virginia driver's license, and transported to a FCPD facility located at 10600 Page Avenue, Fairfax, Virginia 22030, in the Eastern District of Virginia, which is where the Devices are currently located. The Devices have remained at this location since they were

seized from **SOLOMON**'s residence on November 28, 2022. Although FCPD personnel[2] have reviewed the Devices based on the Fairfax County warrant, your affiant has not reviewed any devices pending the execution of this federal search warrant in the abundance of caution.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the devices, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. I submit that there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files

[2] This includes a Fairfax Police Officer who is also a TFO with FBI.

have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and

processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer

accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be

sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

23. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards,

cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

24. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an

individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing log-in information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

25. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques including, but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

26. Based on the information set forth above, I submit that this affidavit supports probable cause to believe that the Devices contain or constitute evidence, fruits, instrumentalities, and/or contraband related to violations of 18 U.S.C. § 2252. I therefore request that the Court issue the proposed search warrant authorizing the examination of the Devices described in Attachment A in order to seek the items described in Attachment B.

Respectfully submitted,

Matthew Lee

Matthew Lee
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to in accordance with
Fed. R. Crim.P. 4.1 by telephone on
January 10, 2023:

Digitally signed by Ivan Davis
Date: 2023.01.10 13:48:47 -05'00'

The Honorable Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched includes the following digital devices and any forensic extractions thereof, which are currently located at the Fairfax County Police Department, 10600 Page Avenue, Fairfax, Virginia 22030, within the Eastern District of Virginia:

1. Dell Latitude laptop computer, serial number HCD9LQ1
2. Jitterbug cellular telephone
3. ASUS Chromebook laptop computer, serial number K6NXCV038893237
4. Three universal serial bus (USB) flash drives
5. Samsung A12 cell phone
6. Western Digital Easystore hard drive, serial number WXP1AC9JKKSP
7. ASUS X541N laptop computer, serial HAN0GR01C57341C
8. 1 Gigabyte (GB) Micro secure digital (SD) card, model PNY
9. AT&T cellular telephone, model V102AA
10. Samsung SGH-A157V cellular telephone, serial number R21D90HMV3R

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Property to be seized

All records and information on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Section 2252—specifically, relating to the distribution, receipt, transportation, possession, and access with intent to view visual depictions of minors engaging in sexually explicit conduct and child pornography—including:

1. Child pornography, visual depictions of minors engaging in sexually explicit conduct, and child erotica or sexualized depictions of children;

2. Any and all records, information, documents, images, videos, communications, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, anonymizing software, encryption software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, contact lists, newsgroup postings by the user, IP addresses assigned, access logs, and any other evidence pertaining to:

   a. Evidence of communication with any minor or minors, information that would assist in identifying those minors, including any images and photographs of children that are or are not sexually explicit;

   b. Images and videos of child pornography, as defined by 18 U.S.C. § 2256, or child erotica, and any information that would assist in identifying minors depicted in such material;

   c. Engaging in sexually explicit activity with children, or the desire or attempt to do

the same by the defendant or any other individual;

d. Textual descriptions of sexually explicit conduct with minors;

e. Who used, owned, or controlled the Electronic Items, including evidence that could help reveal the whereabouts of such person(s);

f. How and when the Electronic Items were accessed or used, to determine the geographic and chronological context of access, use, and events relating to the crime under investigation and to the owner or user of the Electronic Items;

g. The state of mind of the person who used the Electronic Items as it relates to the crime under investigation;

h. Documentation and manuals that may be necessary or helpful to access the Electronic Items or conduct a forensic examination of the Electronic Items;

i. Records or information concerning IP addresses used by the Electronic Items;

j. Diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the computer and internet websites;

k. Correspondence or communications, such as electronic mail, chat logs, and electronic messages;

l. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, accounts, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;

m. Shared images, “friends lists” and “thumbnails”; and

n. Financial records, including credit card information relating to purchases of the

Electronic Items or of any child pornography, visual depictions of minors engaged in sexually explicit conduct, and child erotica or sexualized depictions of children

3. Records and information relating to the use of peer-to-peer file-sharing programs or networks;

4. Evidence of user attribution showing who used or owned the Electronic Items at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

5. Items listed in Attachment A used as an instrumentality of violations of Title 18, United States Code, Section 2252;

6. Evidence of software that would allow others to control the Electronic Items, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

7. Evidence of the lack of such malicious software;

8. Evidence indicating how and when the Electronic Items were accessed or used to determine the chronological context of Electronic Items' access, use, and events relating to the crimes under investigation and to the Electronic Items' user(s);

9. Evidence indicating the state of mind of the user(s) of the Electronic Items as it relates to the crimes under investigation;

10. Evidence of the attachment to the Electronic Items of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Electronic Items;

12. Evidence of the times the Electronic Items were used;

13. Passwords, encryption keys, and other access devices that may be necessary to access the Electronic Items;

14. Records of or information about Internet Protocol addresses used by the Electronic Items;

15. Records of or information about the Electronic Items' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

16. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.